IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TREY PARKER and JESSICA BATISTA, on behalf of themselves and all others similarly situated, Plaintiffs, v. PERSONA IDENTITIES, INC., Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Trey Parker and Jessica Batista, individually and on behalf of all others similarly situated, by their undersigned attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves and their counsel, which are based on personal knowledge.

NATURE OF THE ACTION

1. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant Persona Identities, Inc. ("Persona" or "Defendant") in collecting, capturing, storing, using, otherwise obtaining, possessing, and/or disclosing their and other similarly situated individuals' biometric identifiers[1] and biometric information[2] (referred to collectively at times as "biometrics") without obtaining prior consent and release from Plaintiffs.

2. Defendant markets and sells biometric software that purports to help businesses identify and register consumers, users, or employees.

[1] A "biometric identifier" is any personal feature that is unique to an individual, including fingerprints, iris scans, DNA, and "face geometry."

[2] "Biometric information" is any information captured, converted, stored or shared based on a person's biometric identifier used to identify an individual.

3. Identity verification software is becoming increasingly popular in the digital era, as online businesses often require users to establish their identities by submitting photographs of their driver's licenses or identification cards along with photographs of their faces. Facial landmark data (*i.e.*, biometric identifiers) are then extracted from these photographs and compared to one another. The facial identification software (*e.g.*, Defendant's service) then outputs a "confidence score," which is the probability that—based on the collected facial landmark data—the faces in the two photographs are of the same person.

4. Defendant is the developer of one such facial recognition software, Persona. The Persona software is used to scan uploaded photographs, extract unique biometric identifiers in the form of facial landmark data, and calculate—using the facial landmark data—the probability that the person in a photograph is the same as the person pictured on a drivers' license or other identification card, or the same as the person whose photograph is already in a company database.

5. Businesses can integrate Defendant's software into their own websites or mobile applications so that they can establish a consumer's or user's identity—for example, during a sign up or registration process—without having to send them to another location or webpage.

6. In other words, Defendant's software is designed to be embedded into a business's website or mobile application in such a way that consumers will likely be entirely unaware they are interacting with and providing their sensitive information to an unknown, third-party company, Defendant.

7. Utilizing biometric identification software exposes consumers to serious and irreversible privacy risks, especially here where it is not clear to users that Defendant is collecting their biometric identifiers.

8. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

9. In recognition of these concerns over the security of individuals' biometrics, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Defendant may not obtain and/or possess an individual's biometrics unless it informs that person in writing that biometric identifiers or information will be collected or stored and receives that person's prior consent. *See* 740 ILCS 14/15(b)(1), (b)(3).

10. The BIPA further requires that entities collecting biometrics must inform those persons in writing of the specific purpose and length of term for which such biometric identifiers or biometric information are being collected, stored and used. *See* 740 ILCS 14/15(b)(2).

11. Finally, the entity is expressly prohibited from disclosing, redisclosing, or otherwise disseminating a person's biometrics in the entity's possession without the person's prior consent. *See* 740 ILCS 14/15(d)(1).

12. In direct violation of BIPA §§ 15(b) and 15(d), Defendant collected, stored, used, and otherwise obtained—without first providing notice and obtaining informed written consent—the facial geometry and associated personally identifying information of hundreds or thousands of DoorDash delivery drivers ("Dashers"), who are being required to scan their faces and their photo IDs when signing up for the DoorDash app (the "App"). Defendant further disclosed Dashers' biometrics in its possession to third parties without prior consent.

13. Defendant has been collecting, storing, and disseminating Dashers' facial geometry scans since at least August 2023.

14. Plaintiff Trey Parker signed up to be a DoorDash Dasher in or around August 2023. During the sign up process, Mr. Parker was required to upload a photograph of his ID card, as well as a series of selfies requiring him to turn his face at different angles for verification purposes. Mr. Parker uploaded the required photos and, once he was approved, began driving for DoorDash.

15. Plaintiff Jessica Batista signed up to be a DoorDash Dasher in or around March 2021. In or around January 2024, Ms. Batista attempted to start a shift on the DoorDash App but was told she was required to upload a photo of her ID card, as well as a series of selfies requiring her to turn her face at different angles for verification purposes. Ms. Batista uploaded the required photos and began her shift.

16. Unbeknownst to Plaintiffs and Class Members, when they submitted their photographs to DoorDash, those photographs were in turn sent to Defendant for identity verification purposes. Defendant then extracted the facial landmark data from Plaintiffs' selfies and ID cards (*i.e.*, biometric identifiers), and used this data to calculate the probability that the person in the ID card was the same as the person in the selfies (*i.e.*, biometric information). This "confidence score" was then sent back to DoorDash to confirm that Plaintiffs were who they claimed to be and was stored along with additional information specifically identifying Plaintiffs.

17. In addition, and also unbeknownst to Plaintiffs and Class Members, Defendant disclosed Plaintiffs' biometrics to various third-party vendors, who provided analysis on Plaintiffs' biometrics, maintained backup copies of Plaintiffs' biometrics, and service the systems on which Plaintiffs' biometrics were stored.

18. Defendant never adequately informed Plaintiffs or the Class of the foregoing activities, and never obtained the requisite informed written and prior consent from Plaintiffs or the Class regarding Defendant's biometric collection and disclosures.

19. Plaintiffs bring this action to prevent Defendant from further violating the privacy rights of Illinois residents and to recover statutory damages for Defendant's unauthorized collection, storage, use and dissemination of these individuals' biometrics in violation of BIPA.

THE PARTIES

20. Plaintiff Jessica Batista is, and at all relevant times was, a resident and citizen of Illinois. Ms. Batista has been driving with DoorDash since in or around March 2021, and had her biometrics collected and disclosed by Defendant in or around January 2024.

21. Plaintiff Trey Parker is, and at all relevant times was, a resident and citizen of Illinois. Mr. Parker drove for DoorDash in or around August 2023, and had his biometrics collected and disclosed by Defendant in or around August 2023.

22. Defendant Persona Identities, Inc. is a California corporation with its principal place of business in San Francisco, California. Defendant does business in the State of Illinois.

JURISDICTION AND VENUE

23. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000, exclusive of interest and costs, and at least one member of the proposed class is a citizen of a state different from the state of Defendant.

24. This Court has personal jurisdiction over Defendant. Although Defendant does not put Class Members on notice of its Privacy Policy or procure the consent of Class Members to the same, Defendant's Privacy Policy for Persona Identity Verification—since at least December

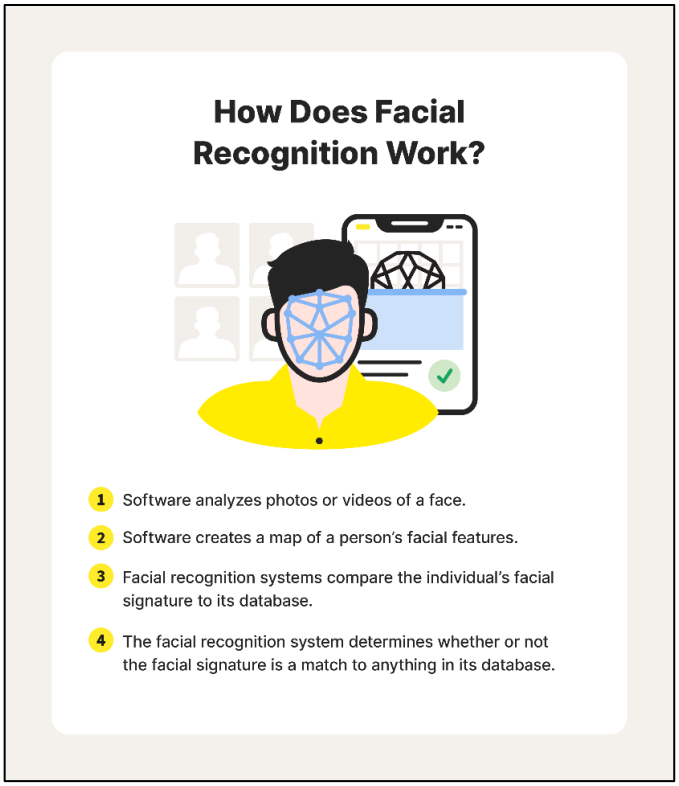
2023—contains a specific section for Illinois residents.[3] Accordingly, Defendant specifically and knowingly targets its biometric collection and disclosure activities at Illinois, and knowingly collects and discloses the biometrics of Illinois residents. Further, Plaintiffs and Class Members had their biometrics captured and collected in Illinois, and were thus harmed in Illinois.

25. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391 because and a substantial part of the events giving rise to Plaintiffs' claims took place within this District.

FACTUAL BACKGROUND

I. Facial Recognition Software Generally

26. In order to understand how Persona collects biometrics in the first place, it is important to understand how facial recognition software works at a high level.

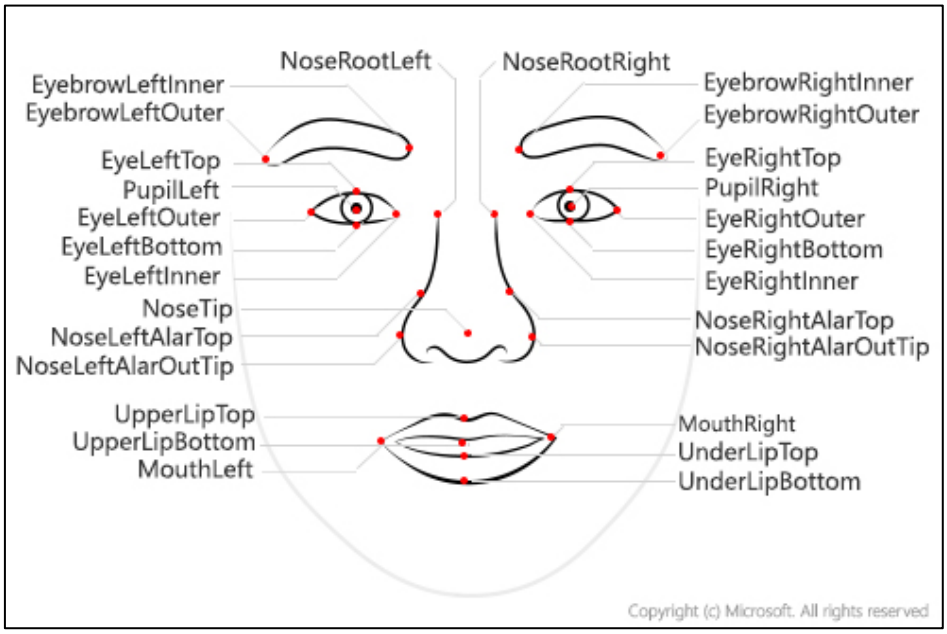


[3] https://withpersona.com/idv-privacy-policy.

27. *First*, a person (*e.g.*, a DoorDash delivery driver) uploads a raw image to the facial recognition software (*e.g.*, Persona). The photograph might be of a person's ID card, such as a driver's license, or other official document that is verified to be of the person. The person does not upload biometrics to the facial recognition software. Instead, the facial recognition software first extracts and creates those biometrics from the image as explained below.

28. *Second*, the facial recognition software analyzes the image for various objects using a "bounding box." The bounding box identifies the various objects in an image or video frame, including but not limited to faces.

29. *Third*, if the facial recognition software detects a face in the image or video frame, it will extract, create, and capture "facial landmark" data, which are the X-Y coordinates of various features of a face used "to create a map of a person's facial features … like their eyes' precise location, scars, or other facial differences."[4] The general "facial landmarks" that a facial recognition software generates are pictured below:



[4] https://us.norton.com/blog/iot/how-facial-recognition-software-works.

30. The X-Y coordinates of the face constitute a person's "facial geometry" and are therefore "biometric identifiers."

31. Again, the photographs are not being sent with biometric identifiers created by the person. Nor is the facial recognition vendor (*e.g.*, Persona) providing a product through which the client (*e.g.*, DoorDash) captures and creates biometric identifiers that are simply stored on the facial recognition vendor's servers (although it is true the biometrics are ultimately stored on the facial recognition vendor's servers). Instead, the photographs are being sent to the facial recognition vendor (Persona), and *the facial recognition vendor itself* (Pesona) is extracting and creating (and thus, capturing and collecting) biometric identifiers from those photographs through its platform. *Rivera v. Amazon Web Services, Inc.*, 2023 WL 4761481, at *5 (W.D. Wash. July 26, 2023) (finding Amazon took an "active step" to collect biometrics where "Plaintiffs allege that Amazon's program, Rekognition, accesses images after they have been uploaded, and extracts the facial geometry of the individuals pictured into a feature vector") (cleaned up).

32. *Fourth*, any "facial geometry" extracted, created, collected, captured, possessed, or otherwise obtained by the facial recognition vendor is stored on the facial recognition vendor's servers. The facial geometry is then associated with a particular individual in the facial recognition vendor's database.

33. *Fifth*, the person (again, in this case, a DoorDash delivery driver) uploads another image to the facial recognition vendor. This second image would be, for instance, a selfie of the person, which will then be compared to the first image to verify the person's identity. The facial recognition vendor again analyzes the second image for any objects and creates and extracts the facial landmark data (facial geometry) from any face it detects.

34. *Finally*, the facial recognition software compares the facial landmark data in the first image to the facial landmark data in the second image and outputs a "confidence score." The "confidence score" is the probability that the two images are of the same person. If the confidence score exceeds a certain threshold, the facial recognition software will return that the two photographs are a match (*i.e.*, that the two photographs are of the same person).

35. Because the facial landmark data is being used to identify a particular person, it constitutes "biometric information."

36. As alleged below, Persona's software works in materially the same way as the process described above. Accordingly, every time a person (*e.g.*, a DoorDash delivery driver) submits a photograph that is sent to Persona for identity verification, Persona creates, collects, captures, stores, and obtains a person's facial landmark data, and thus, a person's biometrics.

II. Defendant's Biometric Verification Software

37. Persona is a technology and AI driven solutions company that aims to "humaniz[e] online identity by helping companies verify that their users are who they say they are."[5] Persona provides verification products and software that allow its customers to verify the identity of their users and employees.[6]

38. Among these products is Selfie Liveness Verification ("SLV"). SLV "protect[s] against identity spoofing by automatically comparing a selfie to the ID portrait with a 3-point composite and liveness checks."[7]

[5] https://withpersona.com/about.

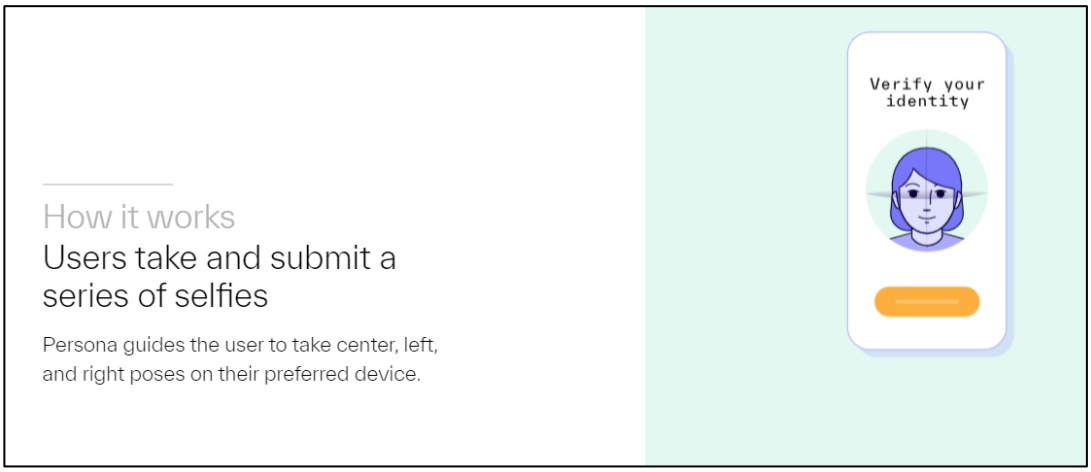
[6] https://withpersona.com/customers.

[7] https://withpersona.com/product/verifications/selfie.

39. Liveness detection typically happens "as soon as the user provides an image, such as a selfie."[8] Liveness detection can leverage data "directly contained within the image itself," including but not limited to "facial measurements"[9] (*i.e.*, facial landmark data).

40. "Selfie verification relies on facial recognition and other related technologies" including liveness detection.[10] Before taking and uploading a selfie, a user is required to first "take a photo of their government-issued ID, such as a driver's license, [] or passport," which "usually forms the bedrock of most verification processes."[11] The ID is then "cross-checked against official databases as well as other user-supplied information to check for discrepancies."[12]

41. Next, "[t]o confirm that the user is in fact the person on the ID, the user is asked to take and submit a selfie or series of selfies."[13]



[8] https://withpersona.com/blog/what-is-selfie-identity-verification-and-how-does-it-work.

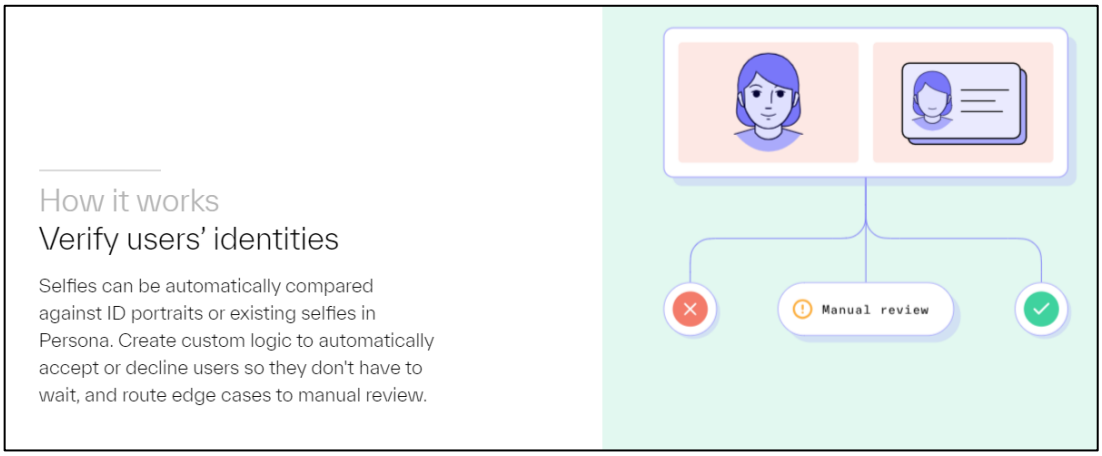
[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] *Id.*



42. Then, the user-submitted selfies or video is then analyzed for liveness detection and cross-checked against the photo in their ID."[14]

43. As Defendant explains on its website, "recent advancements in biometric verification – such as the development of liveness detection – has made verification processes like selfie identity verification more powerful, sophisticated, and secure."[15]

44. As noted above, this "selfie verification" process requires Persona to extract and create "facial landmark data" (*i.e.*, facial geometric/biometric identifiers) from a person's selfie and ID card. Persona then compares the facial landmark data between these two photographs to verify a person's identity (*i.e.*, biometric information).

III. Defendant Violates The BIPA

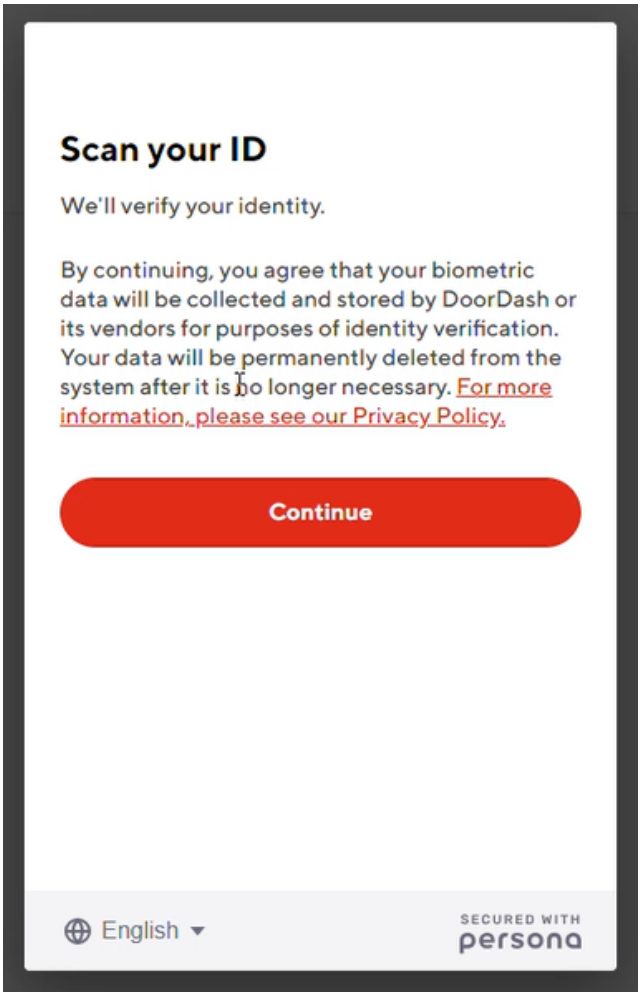
45. In or around 2023, DoorDash partnered with Defendant to verify the identity of its Dashers.

[14] *Id.*

[15] *Id.*

46. When an individual signs up through DoorDash to become a Dasher, they are required to scan their ID for verification purposes. Before continuing to the scan, DoorDash provides Dashers with the following statement on a screen[16]:

> By continuing, you agree that your biometric data will be collected and stored by DoorDash or its vendors for purposes of identity verification. Your data will be permanently deleted from the system after it is no longer necessary. For more information, please see our Privacy Policy.



47. Although the screen includes the language, "secured with persona" in the bottom right corner, this is too inconspicuous for any Dasher to notice. Further, the message states

[16] Screenshot taken from the DoorDash website when signing up to be a Dasher.

"*secured* with persona." The message does not elaborate on what "secured" means, and in no way alerts Dashers that their identities are being verified (and thus, that their biometrics are being collected) by Persona. On the contrary, the message says "*We'll* [i.e., DoorDash will] verify your identity." Moreover, the "secured with persona" statement is no longer on screen once a Dasher continues to the next page.

48. Further, upon clicking the hyperlinked Privacy Policy, Dashers are taken to DoorDash's Consumer Privacy Policy. Prior to February 2, 2024, the Consumer Privacy Policy stated "[t]his Policy *does not apply* to Dashers who deliver orders through the Services ('Dashers'). For the privacy policy for Dashers, please visit the Dasher Privacy Policy."[17] In other words, the hyperlinked privacy policy does not even apply to Dashers, and Dashers are in no way presented with or asked to consent to a privacy policy actually applicable to them.

49. Even if the Consumer Privacy Policy applied to Dashers (and it does not), it would not provide Dashers the proper information required by BIPA in order for Defendant to obtain informed consent to collect and retain biometrics. Prior to February 2, 2024, the Consumer Privacy Policy mentioned biometrics once, but made no mention of who DoorDash's vendors are, nor does it even disclose biometrics are shared with vendors. Persona is also not mentioned once.[18]

50. On February 2, 2024, DoorDash updated its Consumer Privacy Policy. Not only does the new version of the Consumer Privacy Policy not mention biometrics *even once*, there is no hyperlink to the Dasher-specific privacy policy. Nonetheless, the Consumer Privacy Policy still says it "does not apply to Dashers or other contractors." Thus, the current version of the

[17] https://help.doordash.com/legal/document?type=cx-privacy-policy&region=US&locale=en-US (emphasis added).

[18] *Id*.

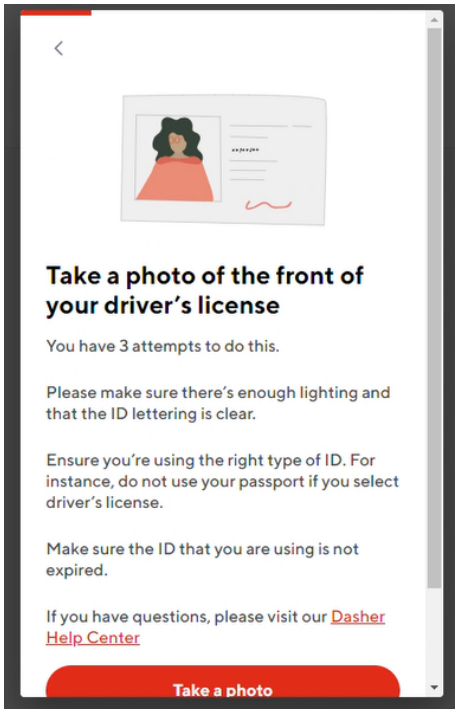
Consumer Privacy Policy gives Dashers even less notice (and less consent) of the wrongful conduct by Persona than before.

51. If Dashers manage to navigate to the Privacy Policy actually applicable to them, there are no provisions mentioning "biometrics," "facial scans," or anything close to informing Dashers that their biometrics/facial geometry are being collected by DoorDash or Persona.[19] Thus, Dashers are not on notice that their biometrics are being collected by Persona.

52. Thus, although there is a blurb that ostensibly informs Dashers that their biometrics are being collected by DoorDash and unspecified vendors, the conflicting information in the Privacy Policies undermine this notice or consent.

53. Once a Dasher selects continue on the screen, the "secured with persona" statement is removed, and Dashers are prompted to take a photo of their ID. The screen also provides a hyperlink to the Dasher Help Center. The Dasher Help Center similarly makes no indication that Persona will be collecting and retaining Dasher's biometrics.

[19] https://help.doordash.com/legal/document?type=dx-privacy-policy&region=US&locale=en-US.



54. Once a Dasher takes a photo of their ID, they are then prompted to take a video selfie, in which they rotate their faces left and right at roughly 35 degrees.[20]

55. Not only are new Dashers subject to these verification requirements, Dashers who signed up prior to DoorDash's implementation of Defendant's software are also required to verify their identities before continuing to deliver for DoorDash.

56. DoorDash's disclosures to Dashers do not give notice that biometrics will be captured, collected, or obtained by Persona.[21]

[20] https://vimeo.com/678365194.

[21] For example, in a YouTube video, a Dasher uploads a photo of the App asking her to verify her identity in which the disclosure reads, "[f]or security purposes, we now require all Dashers to verify their identity to continue dashing. This is a mandatory requirement as outline in our Terms and Conditions and the Dasher ICA." This is not outlined in either the Terms and Conditions or the ICA. https://www.youtube.com/watch?v=-vnXO9NWDN0.

57. Moreover, even after a Dasher has been verified, DoorDash also requires them to submit video selfies for reverification purposes. Defendant collects biometrics from Dashers each time they submit selfie videos for reverification purposes.[22]

58. Defendant's own Privacy Policy—which Dashers are never put on notice of and are never asked to consent to—states "Persona's third party vendors may have access to the Scan Data to provide some or all of the analysis, to store the data, to maintain backup copies, and to service the systems on which such data is stored."[23] Thus, Defendant, without permission, discloses Dashers' biometrics to other third parties.

59. Because, through the identity verification process, Defendant creates, captures, collects, stores, possesses, and otherwise obtains biometrics without a written release or prior consent, Defendant has violated BIPA § 15(b).

60. Further, because Defendant discloses biometrics in its possession to third parties without consent, Defendant has violated BIPA § 15(d).

IV. Plaintiffs' Experiences

A. Plaintiff Parker

61. Plaintiff Trey Parker is a resident and citizen of Island Lake, Illinois. In or around August 2023, Plaintiff Parker applied to be a Dasher for DoorDash through the App.

62. Plaintiff Parker was prompted to upload a photo of his ID, for which he uploaded his license. He then was asked to turn on his front facing camera and position himself in the center. He was then prompted to turn his face slightly to the left and slightly to the right.

[22] https://help.doordash.com/dashers/s/article/Dasher-Identification-Verification-FAQ?language=en_US#How-IDV-Work

[23] https://withpersona.com/idv-privacy-policy.

63. Both of these photographs were submitted to Defendant, who created and extracted Plaintiff Parker's facial landmark data (*i.e.*, his facial geometry or biometric identifiers) from the photographs.

64. Defendant then compared the facial landmark data in the two photographs to calculate the probability that Plaintiff Parker was the person in both photographs, and thus used his biometrics to identify him (*i.e.*, biometric information).

65. Through this process, Defendant came to create, extract, capture, collect, possess, and otherwise obtain Plaintiff Parker's biometrics. Defendant then disclosed Plaintiff Parker's biometrics to third-party vendors to provide some or all of the analysis, to store the data, to maintain backup copies, and to service the systems on which such data is stored.

66. At no time did Plaintiff Parker receive notice from Defendant, in writing or any other form, that Defendant was creating, extracting, capturing, collecting, possessing, or otherwise obtaining his biometrics.

67. At no time was Plaintiff Parker asked by Defendant to provide consent for Defendant to create, extract, capture, collect, possess, or otherwise obtain his biometrics.

68. At no time did Plaintiff Parker consent to Defendant disclosing his biometrics to any other third party.

69. Likewise, Defendant never provided Plaintiff Parker with any opportunity to prohibit or prevent the collection, possession, or disclosure of his biometrics.

70. As a result of the foregoing, Defendant invaded Plaintiff Parker's statutorily protected right to privacy in his biometrics in violation of BIPA §§ 15(b) and 15(d).

B. Plaintiff Batista

71. Plaintiff Jessica Batista is a resident and citizen of Danville, Illinois. In or around March 2021, Plaintiff Batista applied to be a Dasher for DoorDash through the App. Plaintiff Batista has been driving for DoorDash since that time.

72. In or around January 2024, Plaintiff Batista opened the DoorDash App to begin a delivery shift. Upon doing so, Ms. Batista was informed that she must upload a photo of her ID as well as photos of her face in order to continue delivering for DoorDash.

73. Plaintiff Batista uploaded a photo of her license, and was then prompted to open her front facing camera and turn her head left and right to take a selfie for verification.

74. Both of these photographs were submitted to Defendant, who created and extracted Plaintiff Batista's facial landmark data (*i.e.*, his facial geometry or biometric identifiers) from the photographs.

75. Defendant then compared the facial landmark data in the two photographs to calculate the probability that Plaintiff Batista was the person in both photographs, and thus used her biometrics to identify her (*i.e.*, biometric information).

76. Through this process, Defendant came to create, extract, capture, collect, possess, and otherwise obtain Plaintiff Batista's biometrics. Defendant then disclosed Plaintiff Batista's biometrics to third-party vendors to provide some or all of the analysis, to store the data, to maintain backup copies, and to service the systems on which such data is stored.

77. At no time did Plaintiff Batista receive notice from Defendant, in writing or any other form, that Defendant was creating, extracting, capturing, collecting, possessing, or otherwise obtaining her biometrics.

78. At no time was Plaintiff Batista asked by Defendant to provide consent for Defendant to create, extract, capture, collect, possess, or otherwise obtain her biometrics.

79. At no time did Plaintiff Batista consent to Defendant disclosing her biometrics to any other third party.

80. Likewise, Defendant never provided Plaintiff Batista with any opportunity to prohibit or prevent the collection, possession, or disclosure of her biometrics.

81. As a result of the foregoing, Defendant invaded Plaintiff Batista's statutorily protected right to privacy in her biometrics in violation of BIPA §§ 15(b) and 15(d).

CLASS ALLEGATIONS

82. **Class Definition:** Pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3), Plaintiffs bring this action individually and on behalf of a class of similarly situated individuals, defined as follows (the "Class"):

> All Illinois citizens who, during the statute of limitations period, either were Dashers or applied to be Dashers and whose biometric identifiers and/or biometric information were possessed, collected, captured, stored, used, disclosed or otherwise obtained by Defendant.

83. **Numerosity:** The number of persons within the Class is substantial, believed to amount to thousands of persons. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant's records.

84. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which

do not vary from Class Member to Class Member, and which may be determined without reference to the individual circumstances of any class member, include, but are not limited to, the following:

(a) whether Defendant collected or otherwise obtained Plaintiffs' and the Class' biometric identifiers and/or biometric information;

(b) whether Defendant properly informed Plaintiffs and the Class that it collected, used, and stored their biometric identifiers and/or biometric information;

(c) whether Defendant obtained a written release (as defined in 740 ILCS 14/10) to collect, use, and store Plaintiffs' and the Class' biometric identifiers and/or biometric information;

(d) whether Defendant used Plaintiffs' and the Class' biometric identifiers and/or biometric information to identify them;

(e) whether Defendant disclosed, redisclosed, or otherwise disseminated Plaintiffs' and the Class' biometric identifiers and/or information; and

(f) whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

85. **Adequate Representation:** Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation, particularly class actions involving data privacy and/or the BIPA. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Moreover, Plaintiffs are able to fairly and adequately represent and protect the interests of such a Class. Neither Plaintiffs nor their counsel have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiffs have raised viable statutory claims or the type reasonably expected to be raised by members of the Class, and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this Class Action Complaint to include additional Class representatives to represent the Class, additional claims as may be appropriate, or to amend the Class definition to address any steps that Defendant took.

86. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all Class members is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents few management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiffs anticipate no difficulty in the management of this action as a class action. Class-wide relief is essential to compliance with BIPA.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
Violation of BIPA § 15(b),
740 ILCS 14/15(b)

87. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

88. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendant.

89. BIPA § 15(b) makes it unlawful for any private entity to "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless [the entity] first: (1) informs the subject … in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject … in writing of the specific purpose and length of term for which a biometric identifier or biometric information

is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information." 740 ILCS 14/15(b) (emphasis added).

90. Defendant failed to comply with these BIPA mandates.

91. Defendant is a corporation and does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

92. Plaintiffs and Class Members are individuals who had their "biometric identifiers" captured and/or collected by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

93. Plaintiffs' and Class Members' biometric identifiers were used to identify Plaintiffs and Class Members and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

94. Defendant failed to obtain written releases from Plaintiffs and the Class before it created, extracted, captured, collected, and otherwise obtained their biometrics.

95. Defendant failed to inform Plaintiffs and the Class that it was creating, extracting, capturing, collecting, and otherwise obtaining their biometrics before doing so.

96. By collecting, capturing, storing, using, and/or otherwise obtaining Plaintiffs' and the Class's biometrics as described herein, Defendant violated Plaintiffs' and the Class's rights to privacy in their biometrics as set forth in BIPA § 15(b).

97. On behalf of themselves and the Class, Plaintiffs seek: (i) declaratory relief; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA § 15(b)'s requirements for the collection, capture, storage, and use of biometric identifiers and biometric information as described herein; (iii) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA § 15(b) pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent

violation of BIPA § 15(b) pursuant to 740 ILCS 14/20(1); and (iv) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

SECOND CLAIM FOR RELIEF
Violation of BIPA § 15(d),
740 ILCS 14/15(d)

98. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

99. Plaintiffs bring this claim individually and on behalf of the members of the proposed Class against Defendant.

100. BIPA prohibits private entities in possession of biometrics from "disclos[ing], redisclos[ing], or otherwise disseminat[ing] a person's or customer's biometric identifiers or biometric information" without prior consent. 740 ILCS 14/15(d).

101. Defendant failed to comply with these BIPA mandates.

102. Defendant is a corporation and does business in Illinois and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

103. Plaintiffs and Class Members are individuals who had their "biometric identifiers" possessed and disclosed by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

104. Plaintiffs' and Class Members' biometric identifiers were used to identify Plaintiffs and Class Members and, therefore, constitute "biometric information" as defined by BIPA. *See* 740 ILCS 14/10.

105. As alleged above, Defendant came to possess Plaintiffs' and Class Members' biometrics. Defendant then disclosed Plaintiffs' and Class Members' biometrics with third-party vendors to provide some or all of the analysis, to store the data, to maintain backup copies, and to service the systems on which such data is stored.

106. Defendant failed to procure Plaintiffs' and Class Members' prior consent before making said disclosures.

107. By disclosing Plaintiffs' and the Class's biometrics as described herein, Defendant violated Plaintiffs' and the Class's rights to privacy in their biometrics as set forth in BIPA § 15(d).

108. On behalf of themselves and the Class, Plaintiffs seek: (i) declaratory relief; (ii) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA § 15(d)'s requirements for the disclosure of biometric identifiers and biometric information as described herein; (iii) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA § 15(d) pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA § 15(d) pursuant to 740 ILCS 14/20(1); and (iv) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the proposed Class, respectfully seek judgment against Defendant, as follows:

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure, naming Plaintiffs as the representatives of the Class, and naming Plaintiffs' attorneys as Class Counsel to represent the Class;

(b) For an order declaring the Defendant's conduct violates BIPA §§ 15(b) and 15(d);

(c) For an order finding in favor of Plaintiffs and the Class on all counts asserted herein;

(d) For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest in all amounts awarded; and

(f) For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and cost of suit.

JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: February 7, 2024

Respectfully submitted,

By: */s/ Carl V. Malmstrom*

Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 686-0114
E-Mail: malmstrom@whafh.com

BURSOR & FISHER, P.A.
Yitzchak Kopel
Alec M. Leslie*
Max S. Roberts
Caroline C. Donovan*
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Tel: (646) 837-7408
Fax: (212) 989-9163
E-Mail: ykopel@bursor.com
aleslie@bursor.com
mroberts@bursor.com
cdonovan@bursor.com

**Pro Hac Vice Application Forthcoming*

Attorneys for Plaintiffs